No. 16-10109

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ANTONIO GILTON, *et al.*,

Defendants-Appellees.

REDACTED REPLY BRIEF FOR THE UNITED STATES
*** ***PUBLIC VERSION*** ***

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
NO. 3:13-CR-00764 WHO

BRIAN J. STRETCH
United States Attorney

J. DOUGLAS WILSON
Chief, Appellate Division

ANNE M. VOIGTS
Assistant United States Attorney
450 Golden Gate Ave., 11th Floor
San Francisco, CA 94102
(408) 535-5588

Attorneys for Plaintiff-Appellant
UNITED STATES OF AMERICA

December 12, 2016

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

CONSTITUTION AND FEDERAL STATUTES

No. 16-10109

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ANTONIO GILTON, *et al.*,

Defendants-Appellees.

REDACTED REPLY BRIEF FOR THE UNITED STATES
****** PUBLIC VERSION ******

Defendant-appellee Antonio Gilton and amici argue that the government may not obtain historical cell-site location information ("CSLI") from his cellular service provider absent a warrant and probable cause, even though that information did not belong to Gilton, was not maintained for his benefit, and was not stored in a place in which he had a reasonable expectation of privacy. Every court of appeals to have considered the issue has reached the opposite conclusion. This Court should do the same.

Even if a warrant was required, the police obtained one here. In analyzing that warrant's sufficiency, the district court erred as a matter of law by focusing on whether the warrant established probable cause that Antonio Gilton committed the

murder, rather than whether evidence relevant to that murder might be found on his phone. Finally, even if Gilton had a reasonable expectation of privacy in the provider's records and the showing of probable cause in the warrant fell short, the records should nevertheless be admitted under the good-faith exception to the exclusionary rule. Because the district court here erred in granting Gilton's motion to suppress the historical cell-site information obtained from his cell phone carrier through a warrant, this Court should reverse the district court's order.

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT REQUIRE A WARRANT AND PROBABLE CAUSE TO OBTAIN HISTORICAL CSLI, BUSINESS RECORDS CREATED AND KEPT BY CELLULAR SERVICE PROVIDERS FOR THEIR OWN PURPOSES

A. Gilton Has No Reasonable Expectation Of Privacy In Historical CSLI Compiled And Maintained By His Cellular Service Provider

Gilton and amici ignore three key points in contending that a warrant and probable cause is required to obtain historical CSLI from a cellular service provider.

First, they ignore the fact that CSLI belongs to the cellular service provider, not the individual cellphone user. CSLI records are internal business records generated by the provider that identify which cell towers the carrier used to route a user's calls and messages. *United States v. Graham*, 824 F.3d 421, 425-26, 432-33 (4th Cir. 2016) (en banc); *see also United States v. Carpenter*, 819 F.3d 880, 885-

87 (6th Cir. 2016) (noting that wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended).[1] Gilton's focus on "the enormous amount of personal information contained in" cellphones is misplaced because the warrant here did not seek to search his phone. Answering Brief ("AB") at 9-10. Indeed, it did not seek authorization to search anything that belonged to him. Instead, it sought historical CSLI – that is, data collected and maintained by the cellphone service provider at its own discretion for its own business purposes.

Under Supreme Court law, that information belongs to the cellular service provider, not to Gilton. In *United States v. Miller*, 425 U.S. 435, 436, 437-438 (1976), the Court held that the government's acquisition of records maintained by

---

[1] Indeed, cellular service providers inform their users that they do so. *See* http://web.archive.org/web/20120509224057/http:/www.sprint.com/legal/privacy.html?INTNAV=ATG:FT:Privacy; http://web.archive.org/web/20120829032456/http:/www.sprint.com/legal/privacy.html?INTNAV=ATG:FT:Privacy; http://web.archive.org/web/20120330073913/http:/shop2.sprint.com/en/legal/legal_terms_privacy_popup.shtml?ECID=vanity:termsandconditions; http://web.archive.org/web/20120705001309/http:/shop2.sprint.com/en/legal/legal_terms_privacy_popup.shtml?ECID=vanity:termsandconditions. Gilton contends that most customers may not be aware of the terms of service, and that even if they are, those terms do not make it clear that the information may be turned over to law enforcement. But the terms make it clear that they may disclose information in response to legal process or lawful requests. And cellphone users know that they are conveying information to the cellular service provider when using their phones. *See infra.*

defendant's bank and pertaining to his account was not an "intrusion into any area in which [the defendant] had a protected Fourth Amendment interest" because "[o]n their face, the documents subpoenaed here are not [the defendant's] private papers." *Id*. at 440 (internal quotation marks omitted). He could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." *Id*. Nor could Miller claim a "reasonable expectation of privacy" in the records of his transactions with a third party. *Id.* at 442-43.

"This Court," it explained, "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443 (citing *United States v. White*, 401 U.S. 745, 751-52 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); and *Lopez v. United States*, 373 U.S. 427 (1963)); *see also Smith v. Maryland*, 442 U.S. 735 (1979). The Court added that, "even if the banks could be said to have been acting solely as Government agents" in light of the fact that the Bank Secrecy Act required the banks to maintain the records, that would not change the Fourth Amendment analysis. *Miller*, 425 U.S. at 443.

As with the bank records in *Miller*, Gilton "can assert neither ownership nor possession" of the records at issue here; they are Sprint's own "business records" that Sprint created for its own purposes. *Miller*, 425 U.S. at 440. Indeed, the

records here are not even documents that Gilton submitted to Sprint, nor did the government require Sprint to keep those records. *See Miller*, 425 U.S. at 442-43. Instead, they are records that Sprint created for its own business purposes as part of providing telephone service to its customers.

And, under well-established Supreme Court law, obtaining those types of records does not require a warrant based on probable cause, even when challenged by the party to whom the records belong. *See Miller*, 425 U.S. at 446 (reaffirming the "traditional distinction between a search warrant and a subpoena"); *see also Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 194-95 (1946). Rather, as the Court explained in *Miller*, the Fourth Amendment allows the government to use subpoenas to require the production of "relevant" business records and papers. *Miller*, 425 U.S. at 445-46. Such subpoenas are not subject to the same requirements as a search warrant. *See id.* And it is established law that Gilton cannot invoke his own Fourth Amendment rights to object to the production of records by the third-party subpoena recipient. *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).

Second, Gilton and amici seek to blur the core distinction between the content of personal communications, which may be private, and the information necessary to get those communications from point A to point B, which is not. *Carpenter*, 819 F.3d at 886; *see Ex parte Jackson*, 96 U.S. 727, 733 (1878)

(holding that postal inspectors needed a search warrant to open letters and package, but not to inspect the "outward form and weight" of those mailings including the recipient's name and physical address); *Smith*, 442 U.S. 735 (1979) (requesting that defendant's telephone company install a pen register at its offices to record the numbers dialed from the defendant's home phone not a search within the meaning of the Fourth Amendment). Here, the records of calls and the cell-site information both "fall on the unprotected side of this line" because they "say nothing about the content of any calls." *Carpenter*, 819 F.3d at 887-90. The cell-site records – like mailing addresses, phone numbers, and IP addresses – are information that facilitates personal communications, rather than part of the content of those communications. *Id.*

Gilton does not address this Court's decision in *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008), holding that computer investigative techniques that reveal the to/from addresses of email messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account are not Fourth Amendment searches. Amici, who acknowledge *Forrester*, try to distinguish it by relying on its observation in passing that techniques that might be more intrusive or reveal more content might be entitled to greater protection. But they fail to demonstrate how historical CSLI either is more intrusive or reveals more content than the data at issue in *Forrester*. As this Court acknowledged in

Forrester, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses – "but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed." *Id.* Like IP addresses, this Court noted, "certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms." *Id.* When an individual dials a pre-recorded information or subject-specific line, such as sports-scores, lottery-results or phone-sex lines, the phone number will show that the caller had access to specific content information. *Id.* And yet that routing information can be obtained without a warrant or showing of probable cause.

Approximate location information generated by incoming or outgoing calls is not inherently entitled to greater protection than the information that someone has repeatedly visited a particular website, emailed with particular people, or called certain phone numbers. All may reveal something about the content of the communication. None, when obtained from a third party to whom the individual has voluntarily disclosed that information, requires a warrant or a showing of probable cause. And although these records contained historical cell-site

information for a 37-day period, the information revealed only that Gilton was somewhere within the specified sector of a cell tower when calls were made from or to his phone.

Third, Gilton and amici acknowledge, as they must, that the Supreme Court has repeatedly held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44; *see Forrester*, 512 F.3d at 509 (discussing third-party doctrine). This rule – the third-party doctrine – applies even when "the information is revealed" to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443.

Gilton contends, however, that he did not voluntarily convey CSLI to Sprint because CSLI can be generated by applications running in the background or a cellphone scanning its surroundings. He relies primarily on *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015), *appeal dismissed* (Feb. 5, 2016), which distinguished the uniform line of decisions from other circuits by contending that they dealt only with CSLI generated by making or taking phone calls. But the records the government seek to use in this case are like the records in the Fourth, Fifth, Sixth, and Eleventh Circuit cases, not the records described by the district court in *In re Application*. All the government seeks – and all the records reflect – is CSLI generated by making or

receiving phone calls. In any event, cell-phone subscribers are more than capable of selecting the apps they use, and adjusting the information they provide. And, more fundamentally, they choose to carry a cell phone whose benefit is that the wireless provider can route calls, texts, or emails to them whenever they are in range of a network-connected cell tower. The decision to make use of technology that sends and receives information without being tied to a particular location is voluntary and basic to the subscriber's understanding of the service.

Amici go further, contending that Gilton *never* voluntarily conveyed his location information to his wireless carrier. Specifically, amici contend that there is nothing inherent in placing or receiving a cell phone call that would indicate to callers that they are exposing their location information to their wireless carrier. But any cell phone user who has seen her phone's signal strength fluctuate must know that when she places or receives a call, her phone "exposes" its location to the nearest cell tower and thus to the company that operates the tower. *Carpenter*, 819 F.3d at 888-90; *accord United States v. Davis*, 785 F.3d 498, 511 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015); *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 613-14 (5th Cir. 2013). And, as most users know, cell phones do not work when they are outside the range of the provider company's cell tower network. *Davis*, 785 F.3d at 511. To use his phone to make or receive calls, Gilton had to voluntarily transmit information to Sprint – information that included

data about his approximate location. *See Smith*, 442 U.S. at 744; *see also Graham*, 824 F.3d at 427-28; *Carpenter*, 819 F.3d at 887-89 (holding that "for the same reasons that Smith had no expectation of privacy in the numerical information at issue [in *Smith*], the defendants have no such expectation in the [CSLI] locational information here"); *Davis*, 785 F.3d at 511-13 (holding that defendant has no "objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls").

Gilton and amici rely on the Third Circuit's decision in *In re Application of U.S. for an Order Directing a Provider of Elec. Communication Serv. to Disclose Records to Gov't.*, 620 F.3d 304, 313, 317 (3d Cir. 2010), but there too the appellate court rejected the argument that a warrant and probable cause are invariably required to obtain CSLI. Although the Third Circuit stated that "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information," *id.* at 317 (emphasis omitted), a factual premise the Fifth, Sixth, and Eleventh Circuits have rejected, the court did so only to note the possibility that the government's acquisition of such information could implicate the Fourth Amendment "if it would disclose location information about the interior of a home," *ibid*. (emphasis added); *see id.* at 320 (Tashima, J., concurring in the judgment). Here, nothing suggests that the CSLI would provide that level of specificity.

B. Nothing About The Quantity Or Quality Of The CSLI Changes That Analysis

In essence, Gilton seeks a rule that he has a personal Fourth Amendment interest in a business's record of the service it provided him where that record reveals the approximate location of his phone at a specific point in time. No recognized Fourth Amendment doctrine supports that contention. Nevertheless, Gilton and amici argue that the quantity and quality of information that cellphone users turn over to cellular service providers entitle those users to constitutional protection with respect to the providers' records. They do not.

With respect to the first point, Gilton and amici contend that the more information an individual voluntarily discloses to a third party, the greater the constitutional protections that person is entitled to over the third party's records. Here, they point to the fact that the warrant covered 37 days of Gilton's CSLI generated by calls by and to his phone. But in *Graham*, the court held that neither a warrant nor probable cause were required even though 221 days of records were involved. 824 F.3d at 424-25. And acquiring a longer period of CSLI does not convert that acquisition into a search, any more than acquiring a longer period of bank records converts that acquisition into a search. The third-party doctrine's premise is that exposure of information to – and generation and possession of business information by – a third party is incompatible with a person's reasonable expectation that the information will not be revealed to the government by that

third party. That premise holds true regardless of the quantity of third-party information acquired.

With respect to the quality of the information involved, Gilton and amici argue that historical CSLI allows for inferences as to whether a person is home, revealing otherwise undiscoverable facts about constitutionally protected spaces. Although they contend that Gilton's CSLI can give rise to inferences about where he (or his phone) was at a given point, it does not do so with a level of precision that they imply.[2] Indeed, the precision of CSLI can vary dramatically, but rarely will CSLI be precise enough to place a phone within a specific residence. *United States v. Hill*, 818 F.3d 289, 295 (7th Cir. 2016) (noting that in urban areas, cell towers may be located relatively close together, while cell sites in rural areas may be farther apart); *see United States v. Reynolds*, 626 F. App'x 610, 615 (6th Cir. 2015) (unpublished); *see also Graham*, 824 F.3d at 425, n.3; *Davis*, 785 F.3d at 503-04 ("Nearby" a relative term, ranging from a block (maybe less) to a couple miles (maybe more) depending on the tower density in the area).

[2] Although amici and Gilton have copies of the phone records at issue, the amicus brief is filled with factual assertions regarding the nature of cell-site records that are untethered from the record in this case and which the government believes are fundamentally misleading or false. For example, the government disputes their claims that "[f]or a typical user, over time, some of that [cell-site] data will inevitably reveal locational precision approaching that of GPS," and that "[e]ach call, text message, and data connection to or from a cell phone generates a location record." In any case, such factual claims must be established in the district court by an appropriate fact or expert witness.

Ultimately, Gilton objects to the fact that law-enforcement officers could infer from the cellular service providers' records that Gilton was within a particular radius of a cell tower (and, with sector information, within a particular "pie slice" of that area). But "an inference is not a search." *Kyllo v. United States*, 533 U.S. 27, 33 n.4 (2001). And whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it. *Carpenter*, 819 F.3d at 888; *see Donaldson v. United States*, 400 U.S. 517, 522 (1971) (explaining that the lack of Fourth Amendment protection for third-party business records was "settled long ago"); *id.* at 537 (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others."). "[I]nformation that is not particularly sensitive – say, the color of a suspect's vehicle – might be protected if government agents broke into the suspect's garage to get it. Yet information that is highly sensitive – say, all of a suspect's credit-charges over a three-month period – is not protected if the government gets that information through business records obtained per a subpoena." *Carpenter*, 819 F.3d at 888-89.

Nor is obtaining historical CSLI from a cellular service provider constitutionally analogous to obtaining information from an individual's home through governmental intrusion, be it physical or electronic. Gilton and amici rely on *United States v. Karo*, 468 U.S. 705, 714 (1984), which held that police officers

conducted a Fourth Amendment search when they used a beeper device to monitor the location of a container within a private residence, and *Kyllo,* 553 U.S. at 40, which held that the use of a thermal imaging device "that is not in general public use[] to explore details of the home that would previously have been unknowable without physical intrusion" was also a Fourth Amendment search. But in each case, the use of the device in question permitted the authorities to obtain information from inside a house that had not already been exposed to the public. *See Karo*, 468 U.S. at 714-716; *Kyllo*, 533 U.S. at 34-40. Here, the information was generated not by the government intruding into a house, but by a business (Sprint) collecting and compiling information for its own business purposes regarding the use of its cell towers. And the information was obtained from Sprint, not Gilton. The relevant analogy to that acquisition is not the inside-the-home techniques of surveillance in *Karo* or *Kyllo*, but rather the interview of a witness about a defendant's whereabouts, which has never been understood to qualify as a Fourth Amendment "search" of the home. Indeed, the use of a pen register for a residential phone supports an even stronger inference whether and when an individual is at home, and yet under settled Supreme Court law, it does not require a warrant. *Forrester*, 512 F.3d at 511 (holding that the government's surveillance of e-mail addresses "may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail").

Just because facts about a person can be deduced from records or other information in the possession of a third party does not make the acquisition of that information a Fourth Amendment search of the person. Indeed, none of the cases on which Gilton and amici rely alter that conclusion.

For example, in *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court relied on the fact that the government had "physically intrud[ed] on a constitutionally protected area" – the suspect's automobile – to install and use a Global Positioning System (GPS) tracking device to continuously monitor its movements over the course of 28 days. *Id.* at 949. In holding that the attachment of the device constituted "a classic trespassory search," the majority did not reach the question whether (let alone hold that) tracking a person's vehicle on public streets violates a reasonable expectation of privacy. *See Jones*, 132 S. Ct. at 953-54. *Cf. United States v. Knotts*, 460 U.S. 276, 281-82 (1983) (holding that an individual has no expectation of privacy in his movements on public roads, that the use of a beeper did not alter that conclusion, and that "[n]othing in the Fourth Amendment prohibited the police from augmenting the[ir] sensory faculties . . . with such enhancement as science and technology afforded them in this case"). In this case, by contrast, Gilton does not allege a trespass. Moreover, the GPS tracking device in *Jones* allowed law-enforcement officers to use "signals from multiple satellites" to continuously track the movements of the defendant's vehicle

over the course of 28 days, accurate to "within 50 to 100 feet." 132 S. Ct. at 948. But the information in this case consisted of historical records indicating which of the cellular-service provider's antennas communicated with petitioner's phone only when the phone was making or receiving calls, not continuously. ER 238 n.3. And in *Riley v. California*, 134 S. Ct. 2473, 2485, 2489-90 (2014), there was no question but that the review of the contents of a cell phone constitutes a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. *See id.* at 2482. Nor does this case touch on *Riley*'s central concern: namely, that cell phones may contain "vast quantities of personal information" that could be used to discern "[t]he sum of an individual's private life," including information about the user's health, family, religion, finances, political and sexual preferences, and shopping habits, as well as GPS records of the user's "specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2485, 2489-90. Here, the historical cell-site records obtained in this case would only reveal Gilton's approximate location when calls were made to or from his call. They revealed nothing about the content of his calls or his phone.

C. Even Assuming That Government Acquisition Of CSLI Is A Fourth Amendment Search, A Showing Of Reasonable Relevance To An Investigation, Rather Than Probable Cause, Would Satisfy The Fourth Amendment's Reasonableness Requirement

Even if this Court were to hold (or assume) that the use of government process to acquire CSLI is a "search," the Fourth Amendment would not require a showing of probable cause to justify such process. Despite Gilton's arguments to the contrary, not all Fourth Amendment searches require probable cause. And not all demands for records constitute Fourth Amendment searches. *See Miller*, 425 U.S. at 446 (reaffirming the "traditional distinction between a search warrant and a subpoena"); *see also Oklahoma Press Pub. Co.*, 327 U.S. at 209.

Here, the Stored Communications Act authorizes a phone company to disclose to law enforcement call records and historical cell-site information on receipt of a court order under 18 U.S.C. § 2703(d) supported by a finding that reasonable grounds exist to conclude that the records are relevant and material to an investigation (18 U.S.C. § 2703(c)(1)(B) & (d)). *See In re Application of U.S. for an Order Directing a Provider of Elec. Communication Serv. to Disclose Records to Gov't.*, 620 F.3d at 313 ("this standard is a lesser one than probable cause"). Gilton and amici contend that this is constitutionally inadequate, but neither offers an adequate explanation why the SCA standard is constitutionally unreasonable given that it provides more substantial privacy protections than an ordinary judicial subpoena. Indeed, the SCA raises the bar for obtaining historical

cell-site records, by requiring the government to establish "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[ ] are relevant and material to an ongoing criminal investigation," 18 U.S.C. § 2703(c) and (d) (emphasis added).

The government has a compelling interest in obtaining historical cell-site records without having to meet the requirement of a warrant and probable cause, because, like other investigative techniques that involve seeking information from third parties about a crime, this evidence is "particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects." *See Davis*, 785 F.3d at 518. Society has a strong interest in both promptly apprehending criminals and exonerating innocent suspects as early as possible during an investigation. *See Maryland v. King*, 133 S. Ct. 1958, 1974 (2013); *United States v. Salerno*, 481 U.S. 739, 750-51 (1987). Thus, even if the affidavit did not establish probable cause, at a minimum, the warrant met the lesser Section 2703(d) standard, and that was sufficient to satisfy the Fourth Amendment. *See infra* Section II.

II. EVEN IF PROBABLE CAUSE WAS NECESSARY, THE WARRANT ESTABLISHED A REASONABLE NEXUS BETWEEN THE MURDER AND ANTONIO GILTON'S PHONE

This Court need not reach the question whether the Fourth Amendment requires a warrant and probable cause to obtain historical CSLI because the police

here obtained a warrant, and the district court erred in concluding that that warrant was not adequate.

Gilton argues that the district court did not ignore the evidence [redacted], but cannot point to any part of the order in which the district court refers to that evidence. Instead, he argues, the affidavit did not establish that Gilton was in the Bay Area at the time of the murder, or that every member of the Gilton family was involved in that murder. But neither has to be true for the affidavit to establish a reasonable nexus between the murder and the information on Gilton's phone – in other words, to show "'that it would be reasonable to seek the evidence in the place indicated in the affidavit.'" *United States v. Pitts*, 6 F.3d 1366, 1369 (9th Cir. 1993); *see United States v. Fernandez*, 388 F.3d 1199, 1254 (9th Cir. 2004); *United States v. Chavez-Miranda*, 306 F.3d 973, 978-79 (9th Cir. 2002). It was not necessary for Gilton to be in San Francisco or for every member of the family to have been involved in the murder for it to be reasonable to think that his phone records and CSLI might help determine who in the family was involved.

L.G. stayed with Gilton in Los Angeles, where she met and was pimped out by Sneed. After her mother traveled to Los Angeles to try to persuade her to return to San Francisco, L.G. and Sneed drove to San Francisco and arrived at her parents' home at approximately 4:00 p.m. ER 415-16. Later that same night, L.G.

had an argument with her mother about wanting to return to Los Angeles with Sneed. ER 416. She texted Sneed to pick her up from her parents' home and "used her brother's cell phone charger to charge her phone." *Id.* Although the district court did not acknowledge any of these facts, either explicitly or implicitly,

[redacted] ER 428-29. Moreover, Barry Gilton told the police that he had returned to the house at 12:15 a.m. and gone to his bedroom, when in fact cell records showed that his phone was moving around San Francisco between 12:49 a.m. and 2:19 a.m. on the night of the murder – and near his house around the time of the murder. ER 419. Finally, the shooter's car arrived at around the same time as Sneed, suggesting that the shooter was tipped off by someone at the house about Sneed's arrival. ER 416.

Gilton contends that because the court properly recited the law at the beginning of its order, it therefore correctly applied it. It did not. Instead, the

district court concentrated its analysis on whether the warrant contained information expressly and specifically incriminating Gilton, not whether it would be reasonable to look for evidence related to the murder in those phone records. That was legal error. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 556-57 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought.").

Based on the affidavit, there was no doubt that Sneed was murdered. And there was ample reason to believe that Sneed was targeted by the Gilton family because of his relationship with Antonio Gilton's minor sister, that the shooter did not act alone, and that family members' cell phone records might have useful information about the murder. That was enough to establish a substantial basis to find both probable cause that a crime had been committed and a reasonable nexus between the murder and Antonio Gilton's phone records and CSLI. The district court's contrary conclusion was error.

III. EVEN IF THE WARRANT DID NOT ESTABLISH PROBABLE CAUSE, THE OFFICERS RELIED ON IT IN GOOD FAITH

Even if the district court did not err in concluding that the warrant was inadequate, it erred in holding that the officers did not act in good faith when they relied on the search warrants issued by a neutral and detached judge. *See United*

States v. Leon, 468 U.S. 897, 926 (1984). Gilton contends, however, that the affidavit was too thin to survive even under the good-faith exception.

In the alternative, Gilton contends that the good-faith exception cannot apply because the officer who signed the affidavit failed to use sufficiently affirmative language. In so doing, Gilton attempts to sidestep the actual allegations in that affidavit. There was no doubt that a crime was committed. And the allegations in the affidavit pointed towards the murderers as being related to L.G. Given this, the district court erred in concluding that no officer "could . . . have harbored an objectively reasonable belief in the existence of probable cause." *Leon*, 468 U.S. at 923-26; *see Herring v. United States*, 555 U.S. 135, 145 (2009) (the "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances").

In addition, it was reasonable for the officers to assume that if the trial judge found probable cause, at a minimum the facts in the affidavit satisfied the Section 2703(d) standard ("specific and articulable facts showing that there are reasonable grounds to believe that the [records] are relevant and material to an ongoing criminal investigation") for a court order authorizing the collection of phone records. Thus, even if this Court were to hold that the Section 2703(d) standard does not satisfy the Fourth Amendment, police officers could reasonably rely on a

court order based on evidence that meets the "reasonable grounds" standard, especially where the officers obtained the court order before any appellate court (or for that matter, any district judge in the Northern District of California) had struck Section 2703(d) as unconstitutional. *See Illinois v. Krull*, 480 U.S. 340, 349-50 (1987) (exclusionary rule did not apply where officers acted in "objectively reasonable reliance on statute," even if statute was "subsequently declared unconstitutional"); *United States v. Dorsey*, 2015 WL 847395, at *8 (C.D. Cal. Feb. 23, 2015) (collecting cases applying *Krull* to the collection of historical cell-site information from a phone company).

CONCLUSION

For the reasons stated above, this Court should reverse the district court's order granting Antonio Gilton's motion to suppress.

Dated: December 12, 2016

Respectfully submitted,

BRIAN J. STRETCH
United States Attorney

J. DOUGLAS WILSON
Chief, Appellate Division

/s/ Anne M. Voigts
ANNE M. VOIGTS
Assistant United States Attorney

Attorneys for Plaintiff-Appellant
UNITED STATES OF AMERICA

STATEMENT OF RELATED CASES

Pursuant to Ninth Circuit Rule 28-2.6(a), counsel for Appellant states that there is another interlocutory appeal from the same district court case related to this appeal: *United States v. Williams, et al.*, CA No. 15-10475, which was decided on December 5, 2016.

Dated: December 12, 2016

/s/ Anne M. Voigts
ANNE M. VOIGTS
Assistant United States Attorney

Form 8. Certificate of Compliance Pursuant to 9th Circuit Rules 28-1.1(f), 29-2(c)(2) and (3), 32-1, 32-2 or 32-4 for Case Number 16-10109

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the end of the brief.*

I certify that (*check appropriate option*):

___ This brief complies with the length limits permitted by Ninth Circuit Rule 28-1.1.
The brief is_____words or___pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

_X_ This brief complies with the length limits permitted by Ninth Circuit Rule 32-1.
The brief is 5,550 words or ___pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

___ This brief complies with the length limits permitted by Ninth Circuit Rule 32-2(b).
The brief is _____words or ___pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable, and is filed by (1) ____separately represented parties; (2)___a party or parties filing a single brief in response to multiple briefs; or (3) ____a party or parties filing a single brief in response to a longer joint brief filed under Rule 32-2(b). The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

___ This brief complies with the longer length limit authorized by court order dated_____. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). The brief is words or____pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

___ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2(a) and is _____words or ___pages, excluding the portions exempted by Fed. R. App. P. 32 (f), if applicable. The brief's type size and type face comply with Fed. R .App. P. 32(a)(5) and (6).

___ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 29-2(c)(2) or (3) and is_____words or____pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

___ This brief complies with the length limits set forth at Ninth Circuit Rule 32-4.
The brief is_____words or ____pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Signature of Attorney: /s/ Anne Voigts Date: 12/12/2016
ANNE M. Voigts
Assistant United States Attorney

CERTIFICATE OF SERVICE

I, Hui Chen, certify that I am an employee of the Office of the United States Attorney, Northern District of California, a person over 18 years of age and not a party to the within action. I certify that on December 12, 2016, I electronically submitted the

- **United States' Redacted Reply Brief**
- **United States' Motion to File Its Unredacted Reply Brief Ex Parte and Under Seal and to Place a Redacted Version of the Brief on Public Record**

in the case of *United States v. Antonio Gilton, et al.*, No. 16-10109, with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I further certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system for the above documents. And to the participant listed below, I have mailed the United States' Motion by First-Class Mail, postage prepaid, for delivery within 3 calendar days.

Mark Stuart Goldrosen, Esq.
(Counsel for Antonio Gilton)
Law Office of Mark Goldrosen
255 Kansas Street, Ste. 340
San Francisco, CA 94103

Dated: December 12, 2016

/s/ Hui Chen
Hui Chen, Paralegal